APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/973,769	10/11/2001	Michael C. Dapp	FS-00510 (02890038AA)	7586

181 7590 06/22/2005		EXAMINER	
MILES & STOCKBRIDGE PC		HENEGHAN, MATTHEW E	

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 06/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/973,769	DAPP, MICHAEL C.
	Examiner	Art Unit
	Matthew Heneghan	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *11 October 2001 and 15 September 2004*.
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-24* is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) *1-24* is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☒ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on *11 October 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date *10/11, 2/27, 5/22*.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-24 have been examined.

Information Disclosure Statement

2.   The following Information Disclosure Statements in the instant application have

been fully considered:

IDS filed 11 October 2001.

IDS filed 27 February 2003.

IDS filed 22 April 2003.

Drawings

3.   The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5)

because they include the following reference characters not mentioned in the

description: 101, 215, 229, 303, 305, 409, 411, 413, 428, 450, 460, 609, 619, 621, 623,

833, and 835.

4.   The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5)

because they do not include the following reference sign mentioned in the description:

"309" on page 18, line 5.

5.   Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in

reply to the Office action to avoid abandonment of the application. Any amended

replacement drawing sheet should include all of the figures appearing on the immediate

prior version of the sheet, even if only one figure is being amended. The figure or figure

number of an amended drawing should not be labeled as "amended." If a drawing figure

is to be canceled, the appropriate figure must be removed from the replacement sheet,

and where necessary, the remaining figures must be renumbered and appropriate

changes made to the brief description of the several views of the drawings for

consistency. Additional replacement sheets may be necessary to show the renumbering

of the remaining figures. Each drawing sheet submitted after the filing date of an

application must be labeled in the top margin as either "Replacement Sheet" or "New

Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner,

the applicant will be notified and informed of any required corrective action in the next

Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

6.   Claim 1 is objected to because of the following informalities: Line 9 is indented,

but begins in the middle of the previous limitation.

        Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act

of 1999 (AIPA) and the Intellectual Property and High Technology Technical

Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting

directly or indirectly from an international application filed before November 29, 2000.

Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior

to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

7.   Claims 1, 2, 4, and 8 are rejected under 35 U.S.C. 102(b) as being anticipated by

U.S. Patent No. 5,606,668 to Shwed.

As per claim 1, Shwed discloses a computer (the engine) have a packet filter

module (the data processor). Traffic is diverted to the packet filter, which tests the

packet against the packet filter's rules (i.e. rules that are used to determine abnormal

usage). If a rule is matched, an alert may be issued, which is sent to the computer for

forwarding to the user. This is all user transparent (see column 7, lines 14-47). This system is used on a router (see column 3, lines 44-48).

As per claim 2, such systems inherently use memory buffers for the communications.

Regarding claim 4, the functionality is inherently performed in real-time.

Regarding claim 8, the rules are disclosed as being "security rules." Such rules are implemented to counter potential attacks.

8.   Claims 20 and 22-24 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 6,119,236 to Shipley et al.

As per claim 20, Shipley discloses a system for wherein several methods are disclosed for detecting abnormal usage characteristics (see column 5, line 58 to column 6, line 67). The system user-transparently then reacts by blocking all access to the LAN from a sender which is associated with a security breach (see column 8, lines 4-9 and column 10, lines 25-27).

As per claim 22, the detecting step is performed at the INSD/firewall and the controlling step is performed at whichever node is appropriate (see column 5, lines 1-43).

As per claim 23, the process is inherently performed in real-time.

Regarding claim 24, all modern network implementations having at least the number of nodes as depicted in Figure 1 are inherently capable of supporting at least two sessions (secure or otherwise) between at least two pairs of nodes.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9.   Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S.

Patent No. 5,606,668 to Shwed as applied to claim 1 above, and further in view of U.S.

Patent No. 6,119,236 to Shipley et al.

Shwed does not disclose the isolation of a network node.

Shipley, which is disclosed as being an improvement over Shwed, discloses the

blocking all access to the LAN from a sender which is associated with a security breach

(see column 8, lines 4-9 and column 10, lines 25-27), and further notes that prior art

firewalls are subject to breach by any new and unique methods of circumventing

security (see column 2, lines 56-65).

Therefore, it would be obvious to one of ordinary skill in the art at the time the

invention was made to modify the invention of Shwed by blocking all access to the LAN

from a sender which is associated with a security breach, as discloased by Shipley, as

prior art firewalls are subject to breach by any new and unique methods of

circumventing security.

10.   Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S.

Patent No. 5,606,668 to Shwed as applied to claim 1 above and further in view of U.S.

Patent No. 5,737,526 to Periasamy et al.

Shwed does not discuss the hierarchical relationships among different nodes.

Periasamy discloses a hierarchically-arranged network arrangement wherein

different nodes can be freely arranged among peer networks. Periasamy further

discloses that this reduces broadcast traffic on slow links (see column 2, lines 49-65).

Therefore, it would be obvious to one of ordinary skill in the art at the time the

invention was made to implement the invention of Shwed by using a hierarchically-

arranged network arrangement, as disclosed by Periasamy, to reduce broadcast traffic

on slow links.

11.   Claims 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over

U.S. Patent No. 5,606,668 to Shwed as applied to claim 1 above and further in view of

Kent, RFC 2401, "Security Architecture for the Internet Protocol," 1998.

Shwed does not discuss session construction within a network.

Kent discloses the construction of secure sessions in IP networks, and specifies

packet information having the identification of a communicating node (see examples on

p. 16), and further suggests that this allows for the enforcement of a security policy in an

IP environment (see p.14).

Therefore it would have been obvious to one of ordinary skill in the art at the time

the invention was made to implement the invention of Shwed by supporting secure

packet information having the identification of a communicating node, as disclosed by

Kent, as this allows for the enforcement of a security policy in an IP environment.

12.   Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S.

Patent No. 5,606,668 to Shwed as applied to claim 1 above and further in view of U.S.

Patent No. 6,233,704 to Scott et al.

Shwed does not discuss the remediation of node faults.

Scott discloses a system wherein remedial action by network management is

triggered by a node fault. The membrane topology functions in a manner corresponding

to a firewall (see column 4, line 29 to column 5, line 58). Scott further suggests that as

long as faulty nodes are kept on a network, they can cause damage (see column 1,

lines 47-50).

Therefore it would have been obvious to one of ordinary skill in the art at the time

the invention was made to implement the invention of Shwed by taking remedial action

by network management in the event of a node fault, as disclosed by Scott, since as

long as faulty nodes are kept on a network, they can cause damage.

13.   Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S.

Patent No. 5,606,668 to Shwed as applied to claim 1 above and further in view of U.S.

Patent No. 6,301,668 to Gleichauf et al.

Shwed does not discuss the management of the various nodes.

Gleichauf discloses a system for maintaining a network map having real-time

information for all nodes in a network for assessing network vulnerabilities (see column

7, lines 26-60), and further notes that can more reliably detect policy violations and

patterns of misuse (see column 3, lines 7-13).

Therefore it would have been obvious to one of ordinary skill in the art at the time

the invention was made to implement the invention of Shwed by maintaining a network

map, as disclosed by Gleichauf, in order to more reliably detect policy violations and

patterns of misuse.

14.   Claims 11-13, 15, and 17 are rejected under 35 U.S.C. 103(a) as being

unpatentable over U.S. Patent No. 6,119,236 to Shipley et al. as applied to claim 20

above, and further in view of U.S. Patent No. 5,922,049 to Radia et al.

Regarding claims 11 and 17, the invention of Shipley disallows network access to

users attempting a security breach, i.e. a potential attack (see column 8, lines 8-17); this

can only be done at the point where the user enters the network (such as the router 22

in Figure 1). Shipley does not disclose the use of locking in routers.

Radia discloses that the use of IP address locking, in order to prevent systems

from forging IP addresses to fool the router into incorrectly relearning routes (see

column 3, lines 5-13).

Therefore, it would be obvious to one of ordinary skill in the art at the time the

invention was made to modify the invention of Shipley by using locking in routers, as

disclosed by Radia, in order to prevent systems from forging IP addresses to fool the router into incorrectly relearning routes.

As per claim 12, Shipley discloses the use of RAM for program execution (see column 4, line 45).

Regarding claim 13, all such processing is performed in real-time.

Regarding claim 15, all modern network implementations having at least the number of nodes as depicted in Figure 1 of Shipley are inherently capable of supporting at least two sessions (secure or otherwise) between at least two pairs of nodes.

15.   Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,119,236 to Shipley et al. in view of U.S. Patent No. 5,922,049 to Radia et al. as applied to claim 11 above and further in view of U.S. Patent No. 5,737,526 to Periasamy et al.

Shipley and Radia do not discuss the hierarchical relationships among different nodes.

Periasamy discloses a hierarchically-arranged network arrangement wherein different nodes can be freely arranged among peer networks. Periasamy further discloses that this reduces broadcast traffic on slow links (see column 2, lines 49-65).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Shipley and Radia by using a hierarchically-arranged network arrangement, as disclosed by Periasamy, to reduce broadcast traffic on slow links.

16.   Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S.

Patent No. 6,119,236 to Shipley et al. in view of U.S. Patent No. 5,922,049 to Radia et

al. as applied to claim 15 above and further in view of Kent, RFC 2401, "Security

Architecture for the Internet Protocol," 1998.

        Shipley and Radia do not discuss session construction within a network.

        Kent discloses the construction of secure sessions in IP networks, and specifies

packet information having the identification of a communicating node (see examples on

p. 16), and further suggests that this allows for the enforcement of a security policy in an

IP environment (see p.14).

        Therefore it would have been obvious to one of ordinary skill in the art at the time

the invention was made to implement the invention of Shipley and Radia by supporting

secure packet information having the identification of a communicating node, as

disclosed by Kent, as this allows for the enforcement of a security policy in an IP

environment.

17.   Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S.

Patent No. 6,119,236 to Shipley et al. in view of U.S. Patent No. 5,922,049 to Radia et

al. as applied to claim 11 above and further in view of U.S. Patent No. 6,233,704 to

Scott et al.

        Shipley and Radia do not discuss the remediation of node faults.

Scott discloses a system wherein remedial action by network management is triggered by a node fault. The membrane topology functions in a manner corresponding to a firewall (see column 4, line 29 to column 5, line 58). Scott further suggests that as long as faulty nodes are kept on a network, they can cause damage (see column 1, lines 47-50).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Shipley and Radia by taking remedial action by network management in the event of a node fault, as disclosed by Scott, since as long as faulty nodes are kept on a network, they can cause damage.

18. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,119,236 to Shipley et al. in view of U.S. Patent No. 5,922,049 to Radia et al. as applied to claim 11 above and further in view of U.S. Patent No. 6,301,668 to Gleichauf et al.

Shipley and Radia do not discuss the management of the various nodes.

Gleichauf discloses a system for maintaining a network map having real-time information for all nodes in a network for assessing network vulnerabilities (see column 7, lines 26-60), and further notes that can more reliably detect policy violations and patterns of misuse (see column 3, lines 7-13).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of Shipley and Radia by maintaining

a network map, as disclosed by Gleichauf, in order to more reliably detect policy

violations and patterns of misuse.

19.   Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over U.S.

Patent No. 6,119,236 to Shipley et al. as applied to claim 20 above, and further in view

of U.S. Patent No. 6,295,276 to Datta et al.

The invention of Shipley disallows network access to users attempting a security

breach (see column 8, lines 8-17); this can only be done at the point where the user

enters the network (such as the router 22 in Figure 1). Shipley does not disclose routing

via redundant links.

Datta discloses the use of redundant routers for network access, as it provides

better fault tolerance and higher speed connections to a LAN (see abstract).

Therefore, it would be obvious to one of ordinary skill in the art at the time the

invention was made to modify the network disclosed by Shipley to have redundant

connections at access points, as it provides better fault tolerance and higher speed

connections to a LAN.

Since Shipley's invention demands that a user be denied all access to a network,

one skilled in the art would design the invention to disallow network access on all

redundant routers in the modified configuration.

Conclusion

20.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Matthew E. Heneghan, whose telephone number is

(571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30

AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gregory Morse, can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(703) 872-9306

Any inquiry of a general nature or relating to the status of this application or

proceeding should be directed to the receptionist whose telephone number is (571) 272-

2100.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

MEH

June 14, 2005